UAS Operator Privacy for RemoteID Messages

draft-moskowitz-drip-operator-privacy-06

November 18, 2020

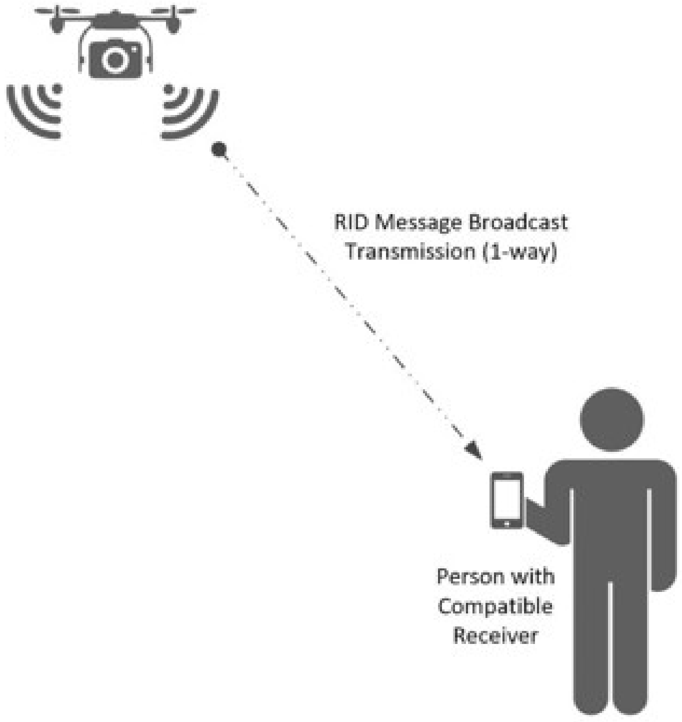
Robert Moskowitz

etal.

From DRIP Charter

The specifications produced by the WG will need to balance public safety authorities’ need to know trustworthy information with UAS operators’ and other involved parties’ privacy.

Private to Whom?



Problem Statement

- The ASTM F3411-19 Standard messages include UAS Operator PII
  - Operator Location and Operator ID
    - Location may be dynamic – changing during Operation
  - In the clear over Broadcast RemoteID
    - Local regulations MAY mandate in the clear, but not everywhere and/or always
  - No spare bytes in messages for ‘standard’ encryption

Encrypt the PII?

- Who has access to PII
  - USS for UAS
  - Authorized Entities
    - Local Public Safety
    - UTM?
      - But who to release to?
    - Others?

How to Encrypt the PII

- UAS SHOULD have business relationship with some USS
  - Thus UAS and USS can share a symmetric key specifically for encrypting PII
  - Authorized entities can ask USS for PII or for key for ongoing realtime access to Operator location PII
    - Can find USS via DRIP RemoteID

How to Encrypt the PII

- Symmetric cipher MUST
  - Encrypt without expanding clear text
    - No bytes to spare
  - Encrypt multiple messages
    - Operator ID Message
    - Operator Location in multiple System Messages
      - Operator moved 1M…

How to Encrypt the PII

- Recommend AES-CFB32 with hidden IV
- Symmetric Key derived via Hybrid ECIES Scheme
    - Key Derivation Function now included
        - Uses KMAC

Why CFB32

- Cipher Feedback mode allows for variable block size like 32 bits
  - NIST SP800-38A
  - 32 bits chosen as size of location fields and ID is multiple of 32
    - Smaller might lead to crypto attack against small changing location
  - Unique IV not needed for each application of CFB

When to Encrypt

- Hiding PII Conditional
  - Only when allowed by USS
    - USS MAY instruct UAS to stop PII protection
  - Only when UAS has connection to USS
    - e.g. loss of Internet connectivity, or no connective in area
    - UAS Time/location change may change USS instructions
  - Otherwise encrypt!

Alternatives to CFB32

- Feistel scheme
  - Slow but pretty neat!
- AES-CTR
  - Needs 2 bytes in message for counter
- Open to discuss other options
  - Time spent taking bruises on CFRG list!
  - NIST Lightweight Crypto (Dec 2021?)

DRIP Requirements met

- PRIV 1 & 2
  - Confidential Handling
  - Encrypted Transport

DRIP Workgroup Action

- CALL FOR WORKGROUP ADOPTION

QUESTIONS ?